

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-236729

(43)Date of publication of application : 31.08.2001

(51)Int.Cl.

G11B 20/10

H04N 5/91

H04N 5/92

H04N 7/167

(21)Application number : 2001-008431

(71)Applicant : HITACHI LTD

(22)Date of filing : 09.04.1999

(72)Inventor : KAWAMAE OSAMU  
TAKEUCHI TOSHIFUMI  
ARAI TAKAO  
KIMURA HIROYUKI  
YOSHIURA YUTAKA

(30)Priority

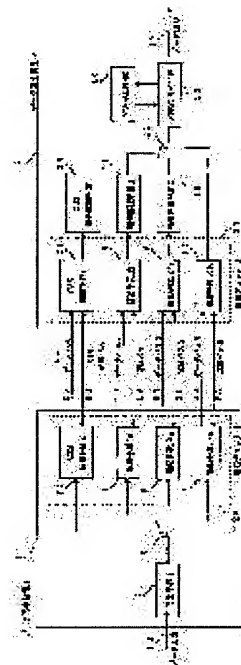
Priority number : 10102386 Priority date : 14.04.1998 Priority country : JP

(54) DATA REPRODUCING METHOD, DATA REPRODUCING DEVICE, DATA ENCODING METHOD, DATA RECORDING METHOD, DATA RECORDING DEVICE, AUTHENTICATION METHOD AND SEMICONDUCTOR CHIP

(57)Abstract:

PROBLEM TO BE SOLVED: To solve the problems that, when the data differently scrambled with recordable recording medium is reproduced, the scrambling is required to be released by discriminating whether the regenerative signals are the signals from which recording media and there is a need for executing respective controls by discriminating whether the kinds of the data are copiable data or copying prohibition data.

SOLUTION: This data recording and reproducing device has a first reproduction processing means which reproduces the data, a second reproduction processing means which receives the data processed by the first reproduction processing and subjects the data to the next reproduction processing, a first authentication means which subjects the first reproduction processing means to authentication and a second authentication means which is the authentication means corresponding to the first authentication means and subjects the second reproduction processing means to authentication. The device described above is provided with plural kinds of the authentication means by having the authentication means different from the first and second authentication means and carries out the authentication meeting the same, thereby releasing the scrambling.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2001-236729  
(P2001-236729A)

(43)公開日 平成13年8月31日(2001.8.31)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H
H 0 4 N 5/91		H 0 4 N 5/91	P
5/92		5/92	H
7/167		7/167	Z

審査請求 未請求 請求項の数38 O L (全 14 頁) 最終頁に続く

(21)出願番号 特願2001-8431(P2001-8431)  
(62)分割の表示 特願平11-102153の分割  
(22)出願日 平成11年4月9日(1999.4.9)  
  
(31)優先権主張番号 特願平10-102386  
(32)優先日 平成10年4月14日(1998.4.14)  
(33)優先権主張国 日本(J P)

(71)出願人 000005108  
株式会社日立製作所  
東京都千代田区神田駿河台四丁目6番地  
(72)発明者 川前 治  
神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内  
(72)発明者 竹内 敏文  
神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内  
(74)代理人 100075096  
弁理士 作田 康夫

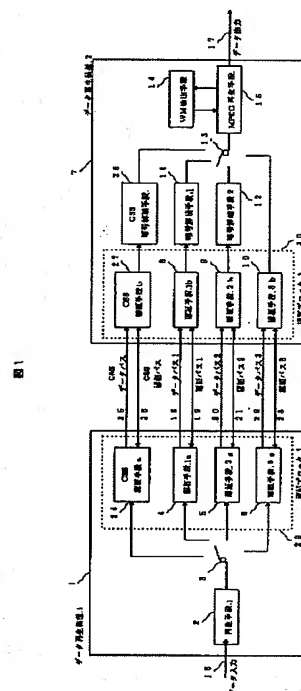
最終頁に続く

(54)【発明の名称】 データ再生方法、データ再生装置、データ符号化方法、データ記録方法、データ記録装置、認証方法及び半導体チップ

(57)【要約】

【課題】 記録可能な記録媒体で異なるスクランブルがかかったデータを再生する場合には、その再生信号がどの記録媒体からの信号かを判別してスクランブルを解除する必要があり、また、データの種類のデータかコピー可能なデータかコピー禁止のデータかを判別して、それぞれの制御を行なう必要がある。

【解決手段】 上記課題は、データを再生する第1の再生処理手段と、第1の再生処理で処理されたデータを受け取り、次の再生処理を行なう第2の再生処理手段と前記第1の再生処理手段に対して認証を行なう第1の認証手段と、第1の認証手段と対応した認証手段で、第2の再生処理手段に対して認証を行なう第2の認証手段とを備えたデータ記録再生装置において、前記第1及び第2の認証手段と異なる認証手段を持つことで複数種の認証手段を備え、それぞれに応じた認証を行い、スクランブルを解除することにより達成される。



## 【特許請求の範囲】

【請求項 1】データを入力して再生し、前記データを外部装置へ出力する再生方法において、データを再生した後、前記外部装置を認識する複数の認証方法のうち、前記再生されたデータの種類に対応した認証方法を選択し、当該選択された認証方法により前記外部装置との認証を行い、前記データを出力することを特徴とするデータ再生方法。

【請求項 2】外部装置から出力されるデータを入力して再生する再生方法において、前記外部装置を認証する複数の認証方法のうち、前記入力されるデータの種類に対応した認証方法により前記外部装置との認証を行い、認証が確認された後に、前記外部装置から出力されるデータを入力し、当該入力されたデータを再生することを特徴とするデータ再生方法。

【請求項 3】互いに認証し合うことによりデータの授受を行って前記データを再生する複数の装置のデータ再生方法であって、前記認証は、複数の認証方法のうち、前記データの種類に対応した認証方法により行うことを特徴とするデータ再生方法。

【請求項 4】データを入力して再生し、データを外部装置へ出力するデータ再生装置において、前記データを再生する再生手段と、前記外部装置との認証を行う複数の認証手段と、当該複数の認証手段から所定の認証手段を選択する選択手段とを有し、当該選択手段は、前記複数の認証手段のうち、前記再生手段により再生されたデータの種類に対応した認証手段を選択し、当該選択された認証手段は、前記外部装置との認証を行い、前記データを出力することを特徴とするデータ再生装置。

【請求項 5】外部装置から出力されるデータを入力して再生するデータ再生装置において、前記外部装置との認証を行う複数の認証手段と、当該複数の認証手段から所定の認証手段を選択する選択手段と、前記データを再生する再生手段とを有し、前記複数の認証手段のうち前記データの種類に対応した認証手段は、前記外部装置との認証を行って当該認証が確認された後、前記データを出力し、前記選択手段は、前記外部装置を認証した認証手段を選択し、前記再生手段は、前記外部装置との認証を行った認証手段が出力したデータを再生することを特徴とするデータ再生装置。

【請求項 6】互いに認証し合うことによりデータの授受を行って前記データを再生する複数のデータ再生装置を有する再生装置であって、前記複数のデータ再生装置は、それぞれ複数の認証手段を有し、前記データの種類に対応した認証手段を選択して、認証し合うことを特徴とする再生装置。

【請求項 7】請求項 4 に記載のデータ再生装置において、

前記複数の認証手段は前記データに含まれた記録媒体の種類を示す情報によって選択されることを特徴とするデ

ータ再生装置。

【請求項 8】請求項 4 に記載のデータ再生装置において、前記複数の認証手段は前記データが映像信号か音声信号か静止画画像信号かプログラムのコードかまたはそのいずれでもないかの種類を示す情報によって選択されることを特徴とするデータ再生装置。

【請求項 9】請求項 4 に記載のデータ再生装置において、

前記複数の認証手段は前記データに含まれたコピーを制御するための情報によって選択されることを特徴とするデータ再生装置。

【請求項 10】請求項 4 に記載のデータ再生装置において、

前記複数の認証手段は前記データに含まれた記録媒体の種類を示す情報とコピーを制御するための情報との組み合わせによって選択されることを特徴とするデータ再生装置。

【請求項 11】請求項 10 に記載のデータ再生装置において、

前記記録媒体の種類を示す情報は、再生専用の媒体か記録可能な媒体かを示す情報を備え、前記コピーを制御するための情報は、コピー制限がないか、コピー禁止か、一世代だけコピー可能かを示す情報を備えていることを特徴とするデータ再生装置。

【請求項 12】請求項 11 に記載のデータ再生装置において、

前記組み合わせは少なくとも、再生専用の媒体であるとの情報と、記録可能な媒体であってかつコピー禁止か一世代だけコピー可能かを示す情報と、記録可能な媒体であってコピー制限がないとの情報という 3 種類の組み合わせを有することを特徴とするデータ再生装置。

【請求項 13】請求項 5 に記載のデータ再生装置は、圧縮された画像データを再生する再生装置であり、当該再生装置はさらに、前記再生手段により再生されるデータに付加された付加情報を検出する検出手段を有することを特徴とするデータ再生装置。

【請求項 14】請求項 13 に記載のデータ再生装置において、

前記再生手段は、前記付加情報がコピー制御のための情報である場合には、当該付加情報にしたがって、前記データの出力を制御することを特徴とするデータ再生装置。

【請求項 15】入力したデータを符号化し、当該符号化したデータを外部装置へ出力するデータ符号化方法において、データを符号化した後、前記外部装置との認証を行う複数の認証方法のうち、前記符号化されたデータの種類に対応した認証方法を選択し、当該選択された認証方法により前記外部装置との認証を行い、前記データを出力することを特徴とするデータ符号化方法。

【請求項 16】外部装置から出力されるデータを入力して記録する記録方法において、前記外部装置との認証を行う複数の認証方法のうち、前記データの種類に対応した認証方法により前記外部装置を認証し、認証が確認された後に、前記外部装置から出力されるデータを入力し、当該入力されたデータを記録することを特徴とするデータ記録方法。

【請求項 17】互いに認証し合うことによりデータの授受を行って前記データの記録を行う複数の装置のデータ記録方法であって、前記認証は、複数の認証方法のうち、前記データの種類に対応した認証方法により行うことを特徴とするデータ記録方法。

【請求項 18】入力したデータを符号化し、当該符号化したデータを外部装置へ出力するデータ符号化装置において、前記入力したデータを符号化する符号化手段と、前記外部装置との認証を行う複数の認証手段と、当該複数の認証手段から所定の認証手段を選択する選択手段とを有し、当該選択手段は、前記複数の認証手段のうち、前記符号化手段により符号化されたデータの種類に対応した認証手段を選択し、当該選択された認証手段は、前記外部装置との認証を行い、前記符号化されたデータを出力することを特徴とするデータ符号化装置。

【請求項 19】外部装置から出力されるデータを入力して記録するデータ記録装置において、前記外部装置を認証する複数の認証手段と、当該複数の認証手段から所定の認証手段を選択する選択手段と、前記データを記録する記録手段とを有し、前記複数の認証手段のうち前記外部データの種類に対応した認証手段は、前記外部装置との認証を行って当該認証が確認された後、前記データを出力し、前記選択手段は、前記外部装置との認証を行った認証手段を選択し、前記記録手段は、前記外部装置との認証を行った認証手段が出力したデータを記録することを特徴とするデータ記録装置。

【請求項 20】請求項 18 に記載のデータ符号化装置及び請求項 19 に記載のデータ記録装置から成る記録装置において、前記請求項 18 に記載のデータ符号化装置の認証手段と、前記請求項 19 に記載のデータ記録装置の認証手段とが、互いに認証し合うことによりデータの授受を行って当該データを記録することを特徴とする記録装置。

【請求項 21】請求項 18 に記載のデータ符号化装置において、前記複数の認証手段は記録対象となる記録媒体の種類を示す情報によって選択されることを特徴とするデータ符号化装置。

【請求項 22】請求項 18 に記載のデータ符号化装置において、前記複数の認証手段は記録するデータのコピーを制御するための情報によって選択されることを特徴とするデータ符号化装置。

【請求項 23】請求項 18 に記載のデータ符号化装置に

において、

前記複数の認証手段は記録する記録媒体の種類を示す情報と、記録するデータのコピーを制御する情報の組み合わせによって選択されることを特徴とするデータ符号化装置。

【請求項 24】請求項 23 に記載のデータ符号化装置において、

前記複数の認証手段は、前記記録媒体の種類を示す情報と記録するデータのコピーを制御する情報との組み合わせに対応した暗号化処理を行なう暗号化処理手段をそれぞれ備えたことを特徴とするデータ符号化装置。

【請求項 25】請求項 23 に記載のデータ符号化装置において、

前記記録媒体の種類を示す情報は、再生専用の媒体が記録可能な媒体かを示す情報を備え、前記記録するデータのコピーを制御する情報は、コピー制限がないか、コピー禁止か、一代だけコピー可能かを示す情報を備えていることを特徴とするデータ符号化装置。

【請求項 26】請求項 25 に記載のデータ符号化装置において、

前記組み合わせは少なくとも、記録可能な媒体であってかつコピー禁止か一代だけコピー可能かを示す情報と、記録可能な媒体であってコピー制限がないとの情報という 2 種類の組み合わせを有することを特徴とするデータ記録装置。

【請求項 27】請求項 18 に記載のデータ符号化装置は、画像データを符号化し圧縮する符号化装置であり、当該符号化装置はさらに、前記符号化手段により符号化されるデータに付加された付加情報を検出する検出手段を有し、

前記認証手段は、当該検出手段によって検出された付加情報にしたがって、前記符号化されたデータの出力を制御するようにしたことを特徴とするデータ記録装置。

【請求項 28】データベースを介して、データの受け渡しを行う複数のデータ処理手段を備えたデータ処理装置において、

前記複数のデータ処理手段は、それぞれ複数の認証手段を備え、前記受け渡しを行うデータの種類に対応した認証手段により前記データ処理手段相互の認証を行うことを特徴とするデータ処理装置。

【請求項 29】請求項 28 に記載のデータ処理装置において、

前記認証手段は、前記データの受け渡しを行う前に、前記認証を行い、全てに認証が成功しない場合には、前記データベースにデータを出力することを停めるようにしたことを特徴とするデータ処理装置。

【請求項 30】請求項 28 に記載のデータ処理装置において、

前記認証手段は、前記データの受け渡しを行う前に、前記データの種類に対応した認証を行い、一部認証が成功

しないデータ処理手段がある場合には、データベースに出力するデータを停めることを特徴としたデータ処理装置。

【請求項 3 1】請求項 2 8 に記載のデータ処理装置において、

前記認証手段は、前記データの受け渡しを行う前に、前記データの種類に対応した認証を行い、一部認証が成功しないデータ処理手段がある場合には、データベースに出力するデータの種類の制限することを特徴としたデータ処理装置。

【請求項 3 2】請求項 2 8 に記載のデータ処理装置において、

前記認証手段は、前記データの受け渡しを行う前に、前記データの種類に対応した認証を行い、一部認証が成功しないデータ処理手段がある場合には、データベースに出力するデータの種類の認証が成功した装置だけに制限することを特徴としたデータ処理装置。

【請求項 3 3】請求項 2 8 に記載のデータ処理装置において、

前記認証手段は、前記データの受け渡しを行う前に、前記データの種類に対応した認証を行い、一部認証が成功しないデータ処理手段がある場合には、データベースに出力するデータがコピー制限の無い情報である場合にだけ出力するようにしたことを特徴としたデータ処理装置。

【請求項 3 4】相互にデータを授受する複数の装置の認証方法であって、複数の認証方法のうち、前記データの種類に対応した認証方法を選択して、相互の前記装置を認証することを特徴とする認証方法。

【請求項 3 5】請求項 4 に記載のデータ再生装置において、前記再生手段と前記認証手段と前記選択手段は、同一のチップに設けたことを特徴とする半導体チップ。

【請求項 3 6】請求項 2 に記載のデータ再生方法であって、前記入力されるデータが暗号化されている場合に、複数の暗号解読方法のうち、前記認証方法に対応した暗号解読方法により、前記データの暗号を解除することを特徴とするデータ再生方法。

【請求項 3 7】外部装置から出力される暗号化されたデータを入力して再生するデータ再生装置において、前記外部装置との認証を行う複数の認証手段と、前記暗号化されたデータの暗号を解除する暗号解読手段であって各々の前記認証手段に対応して設けられた複数の暗号解読手段と、前記暗号解読手段により暗号が解除されたデータを再生する再生手段とを有し、前記複数の認証手段のうち前記暗号化されたデータの種類に対応した認証手段は、前記外部装置との認証を行い、当該認証が確認された後、当該認証手段と対応した前記暗号解読手段に対して前記データを出力し、前記認証手段と対応した暗号解読手段暗号解読手段は、前記認証手段から出力された前記暗号化されたデータを入力して暗号を解除し、当該暗号が解除されたデータを出力することを特徴とするデー

タ再生装置。

【請求項 3 8】暗号化されたデータを入力して再生するデータ再生装置であって、前記暗号化されたデータの暗号を解除する複数の暗号解読手段と、前記暗号解読手段により解読されたデータを再生する再生手段とを有し、前記複数の暗号解読手段のうち、前記暗号化されたデータの種類に対応した暗号化手段は、前記暗号化されたデータの暗号を解除することを特徴とするデータ再生装置。

10 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は画像や音声データを再生する再生装置に関わり、特に記録媒体をコピー管理情報によって再生及び／又は記録を制御するデータ再生装置及びデータ記録装置に関する。

【0002】

【従来の技術】DVD-ROMはCD-ROMの約7倍の容量を持つ媒体である。これにはPC用のプログラムコードだけでなく、映像や音声データを圧縮することで映画ソフトを記録することもできる。DVDにデータを記録する記録媒体としてはDVD-RAMや、DVD-R、DVD-RWがある。これらにも大容量のデータを記録することが出来るため、映画などのソフトウェアがそのままデジタルコピーされることを防止しなければならない。このため、不正コピー防止技術が重要になる。この技術は、日経BP社「日経エレクトロニクス」(1997.8.18 P110～P119)に記載されている。

【0003】DVD-Videoディスクに記録されている映画などは通常CSS (content scrambling system) 方式で暗号化されており、ディスクのデータをコピーしてもこれをデスクランブルしない限り再生できない。

【0004】

【発明が解決しようとする課題】しかし、これにはDVD-Videoディスクのように、もともとデータが記録されているメディアの再生については記載されているが、ユーザーが記録可能な記録媒体の再生については記載されていない。

【0005】記録可能な記録媒体で異なるスクランブルがかかったデータを再生する場合には、その再生信号がどの記録媒体からの信号かを判別してスクランブルを解除する必要がある、また、データの種類の複製可能なデータかコピー禁止のデータかを判別して、それぞれの制御を行なう必要がある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明は、データの種類に対応した認証をするために複数の認証手段を有し、データの種類に対応して認証手段を切替えることにより装置間の認証をおこなうことを特徴とするデータ再生方法、データ再生装置、データ

符号化方法、データ記録方法、データ記録装置、データ記録再生装置、認証方法及び半導体チップを提供するものである。

【0007】

【発明の実施の形態】以下、本発明の実施例を図面を用いて説明する。

【0008】図1は本発明によるコピー制御情報を含むデータを再生する再生装置の一実施例を示したものである。本実施例は例えばDVDのような記録再生可能な媒体について示すが、勿論これは光ディスクに限定するものではなく、データを蓄える媒体全般にあてはまる。

【0009】同図において、1はデータ再生装置1、2は再生手段1、3は切り替えSW1、4は認証手段1 a、5は認証手段2 a、6は認証手段3 a、7はデータ再生装置2、8は認証手段1 b、9は認証手段2 b、10は認証手段3 b、11は暗号解読手段1、12は暗号解読手段2、13は切り替えSW2、14はWM検出手段、15はMPEG再生手段、16はデータ入力、17はデータ出力、18はデータバス1、19は認証バス1、20はデータバス2、21は認証バス2、22はデータバス3、23は認証バス3、24はCSS認証手段a、25はCSSデータバス、26はCSS認証バス、27はCSS認証手段b、28はCSS暗号解読手段、29は認証ブロック1、30は認証ブロック2、である。

【0010】本システムの動作を図1及び図2を用いて説明する。

【0011】ディスクから例えばDVDドライブのようなデータ再生装置1によって読み出されたデータ入力16は、再生手段1により記録されたフォーマットにしたがって復号される。この時、データの種別、例えばデータ中に含まれている記録媒体の種別を示すコード（例えば、再生専用か、記録可能かを示すコード）や、そのデータの構造がスクランブルがかかった構造かを示すコードや、ビデオデータかオーディオデータやコピー制限を示すコード（例えば、コピー許可か、一代コピー可能か、コピー禁止かを示すコード）を読取る。また、光ディスクの場合にはディスクのトラッキング信号から記録媒体の種別を判別する場合もある。ここで、読取ったこれらの情報から切り替えSW1(3)を切り替えて、どの認証手段を用いるかを選択する。認証はデータの受け渡しを行う相手を確認するために、暗号を解くための鍵情報のやり取りをする。この鍵により受け渡されるデータに暗号をかけられており、その鍵を用いて暗号を解読するようにして、データを保護する。

【0012】認証手段1 aが例えば再生専用の記録媒体の認証を行なう手段であり、認証手段2 aが記録可能な記録媒体で、コピー制限情報によりコピーが制限されているものの認証を行なう手段であり、認証手段3 aが記録可能な記録媒体で、コピー制限情報によりコピーが制限されていないものの認証を行なう手段であるとする。

CSS認証手段a(24)は現行のCSS (content scrambling system) に対応したDVDドライブ用の認証手段であり、ここで、本実施例では、CSS認証手段a(24)を独立に記載したが、これは認証ブロック1(29)のように新たな認証手段1 a、2 a、3 aとともにまとめることも出来る。

【0013】データ再生装置2は例えばMPEGデータをデコードするMPEGボードであるとする。認証手段1 bは認証手段1 aに対応した関係にあり、認証バス1(19)を用いて認証の確認を行ない、対応したものでなければそれぞれのスクランブルを解除するための方法が受け渡されないだけでなく、データバス1(18)からのデータの出力を行なわないようにする。認証手段2 b、3 bについても同様に認証手段2 a、3 aに対応した関係にあり、対応したものでなければ認証が行われず、データの出力も止められる。ここでは、説明をわかりやすくするために3組の認証手段の認証を行なうための認証バスと、それぞれからデータを伝送するデータバスを独立としたが、1系列で切り替えながら用いることも可能である。CSS認証手段b(27)は現行のCSSに対応したMPEGボード用の認証手段であり、ここで、本実施例では、CSS認証手段b(27)を独立に記載したが、これは認証ブロックb(30)のように新たな認証手段1 b、2 b、3 bとともにまとめることも出来る。

【0014】再生装置1から再生装置2へデータバス1で伝送されるデータは、伝送の途中でのコピーを防止するためにスクランブルがかけられた状態でデータを伝送する。スクランブルの種類は、再生専用の記録媒体のデータと、記録可能な記録媒体で、コピー制限情報によりコピーが制限されているもののデータと、異なる種類でスクランブルがかけられており、記録可能な記録媒体で、コピー制限情報によりコピーが制限されていないもののデータについてはコピー防止をする必要がないので、スクランブルはかけられていない。そのため、再生装置1からは、認証手段によって記録媒体の種類とデータのスクランブル状態が伝送されることになる。ここで、コピー制限無しのディスクについては、コピー防止のためのスクランブルをかける必要はないが、その場合だけ認証を行なわないようにすると、コピー制限無しと同じコピー制御状態で違法に複製されたディスクを検出することが困難になるため、コピー制限無しのディスクについても認証を行なうようにする。

【0015】認証が確認されるとそれぞれのスクランブルをかけられた状態でデータが伝送される。認証手段によって伝送された記録媒体の種類とデータのスクランブル構造に応じてデータが伝送されるデータバスが選択され、それに応じた暗号解読手段1(11)または暗号解読手段2(12)が動作して、デスクランブルされ切り替えSW2(13)によってMPEG再生手段(15)に送られる。ウォーターマーク検出手段(14)は、MPEG再生

手段(15)でデコードされたデータに埋め込まれた付加情報を検出する検出手段の例であり、本実施例では付加情報としてウォーターマークを検出し、コピー制御情報が検出された場合にはそれにしたがって、データの出力を制御する。本実施例ではMPEG再生手段(15)を制御してデータの出力を制御する一例を示したが、制御方法は、出力データを止めたり、データをバス上で破壊するなど、これに限られるものではない。

【0016】ここで、再生手段1と切り替えSW1(3)、認証手段1a(4)、認証手段2a(5)、認証手段3a(6)は同一のLSI内に組み込むことにより、データを途中から取り出すことを困難にし、認証手段1b(8)、認証手段2b(9)、認証手段3b(10)、暗号解読手段1(11)、暗号解読手段2(12)、切り替えSW2(13)、とWM検出手段(14)、MPEG再生手段(15)を同一のLSI内に組み込むことにより、データを途中から取り出すことを困難にする。

【0017】図2は本発明によるデータ再生装置をDVDドライブ装置に当てはめた場合を示したものである。本実施例は例えばDVDのような記録再生可能な記録媒体について示すが、勿論これは光ディスクに限定するものではなく、記録再生可能な媒体全般にあてはまる。

【0018】同図において、24はDVDディスク、25はDVDドライブ、26はピックアップ、27はプリアンプ、28はシステム制御手段1、29はMPEG再生ボード、30はシステム制御手段2、31はコンバータ、32はモニタ、である。

【0019】DVDディスク(24)からピックアップ(26)で読み出された信号はプリアンプ(27)を介してデータ再生装置1(1)に入力される。データ再生装置1(1)はシステム制御手段1(28)により制御され、動作の状態を決定する。ここまでのDVDドライブ(25)の主な動作である。データ再生装置1(1)で再生された信号は、データ再生装置2(7)に伝送される。データ再生装置2(7)はシステム制御手段2(30)により制御され、動作の状態を決定する。データ再生装置2(7)で再生されたデータはコンバータ(31)で変換されて、モニタ(32)に出力し映像が映し出される。ここまでのMPEG再生ボード(29)の主な動作である。

【0020】図3は本発明の記録媒体の種類とデータのスクランブル構造が記録されたコードを含むデータの一例として、DVDのセクタデータの構成を示したものである。DVDではメインデータ2048バイトの前にIDと呼ばれる識別データや、CPR\_MAIと呼ばれる著作権管理情報が書かれている。

【0021】著作権管理情報(CPR\_MAI)には、著作権管理情報及び地域管理情報の両者に対応している。リードインエリアにおいては、著作権保護システムの特定データ構造(スクランブル構造に相当する)を持つか持たないか、指定された地域で再生してよいかい

ないかを記述している。データ領域では、そのセクタが著作権を有する素材を含むか含まないか、著作権保護システムの特定データ構造を持つか持たないか、コピー制限があるか(コピー許可、一世代コピー可能、コピー禁止)を記述している。

【0022】図4はDVDの識別(ID)データの構成を示したものである。IDはセクタ情報を構成する最初の4バイトの中にデータタイプと呼ばれる再生専用データか、追記用データと書換用データのための予備を示すコードがある。

【0023】セクタフォーマットタイプには再生専用ディスク及び追記用ディスクに規定されたCLVフォーマットタイプか、書換用ディスク用に規定されたゾーンフォーマットタイプかが記録されている。領域タイプには、データ領域、リードイン領域、リードアウト領域、再生専用ディスクのミドル領域かが記録されている。データタイプには、再生専用データか追記用データ(リンクデータ)と書換用データのための予備とされている。

【0024】図5は本発明によるコピー制御情報を含むデータを記録する記録装置の一実施例を示したものである。本実施例は例えばDVDのような記録再生可能な記録媒体について示すが、勿論これは光ディスクに限定するものではなく、記録再生可能な媒体全般にあてはまる。

【0025】同図において、51はデータ記録装置2、52は記録手段1、53は切り替えSW4、55は認証手段2d、56は認証手段3d、57はデータ記録装置1、59は認証手段2c、60は認証手段3c、62は暗号化手段2、63は切り替えSW3、64はWM検出手段、65はMPEG符号化手段、66はデータ出力、67はデータ入力、70はデータバス2、71は認証バス2、72はデータバス3、73は認証バス3である。

【0026】ディスクからDVDドライブのようなデータ再生装置1によって読み出され、モニタに出力された映像データ等を入力とするデータ入力(67)は、記録手段1(52)によりデジタルデータに変換され記録するためのフォーマットにしたがって符号化される。この時、データの種類、例えば、記録媒体の種類を示すコード(例えば、再生専用か、記録可能かを示すコード)をフォーマットにしたがって書き込む。また、他のデータの種類として、例えば、コピー制御により暗号化(スクランブル)をかけるデータ構造かを示すコードや、コピー制限を示すコード(例えば、コピー許可か、一世代コピー可能か、コピー禁止かを示すコード)を書き込む。次に、そのデータがコピー制御を行なう必要があるデータであるならば、その記録媒体と、コピー制御の状態に応じたスクランブルを施す。ここで、コピー制御情報から切り替えSW3を切り替えて、どの認証手段を用いるかを選択する。

【0027】ウォーターマーク検出手段64では、MP



EG符号化手段65に入力されたデータに付加された付加情報であるコピー制御情報を検出して、その情報に従って制御を行なう。例えば、検出された情報がコピー禁止の情報であれば、記録データを出力することを止め、コピー制限無しのデータであるならば、スクランブルを行わずに符号化処理を行なうようにする。本実施例ではMPEG符号化手段65を制御してデータの出力を制御する一例を示したが、制御方法は、出力データを止めたり、データをバス上で破壊するなど、これに限られるものではない。

【0028】認証手段2cが、記録可能な記録媒体であってコピー制限情報によりコピーが制限されているものの認証を行なう手段であり、認証手段3cが、記録可能な記録媒体であってコピー制限情報によりコピーが制限されていないものの認証を行なう手段であるとする。

【0029】また、本実施例には省略したが、再生装置と同様に現行のCSSに対応した認証手段が含まれる場合もあり、これとあわせて認証ブロックとすることも可能である。

【0030】データ記録装置1は例えばMPEGデータをエンコードするMPEGボードである。認証手段2dは認証手段2cに対応した関係にあり、71認証バス2を用いて認証の確認を行ない、対応したものでなければそれぞれのスクランブルを解除するための方法が受け渡されないだけでなく、70データバス2からのデータの出力を行なわないようにする。認証手段3dについても同様に認証手段3cに対応した関係にあり、対応したものでなければ認証が行われず、データの出力も止められる。ここでは、説明をわかりやすくするために2組の認証手段の認証を行なうための認証バスと、それぞれからデータを伝送するデータバスを独立としたが、1系列で切り替えながら用いることも可能である。

【0031】データ記録装置1からデータ記録装置2へデータバス2で伝送されるデータは、伝送の途中でのコピーを防止するためにスクランブルがかけられた状態でデータを伝送する。コピー制限情報によりコピーが制限されていないもののデータについてはコピー防止をする必要がないので、スクランブルはかけられていない。

【0032】そのため、データ記録装置1からは、認証手段によってデータのスクランブル状態が伝送されることになる。切り替えSW3(63)はそのデータに応じた暗号化手段2または暗号化手段を通らないパスのどれかを選択し、データに応じたスクランブルがかけられるようにする。

【0033】認証が確認されるとそれぞれのスクランブルをかけられた状態でデータが伝送される。認証手段によって伝送された記録媒体の種類とデータのスクランブル構造に応じてデータが伝送されるデータバスが選択され、切り替えSW4(53)によって記録手段1(52)に送られる。

【0034】ここで、認証手段2c(59)、認証手段3c(60)、暗号化手段2(62)、切り替えSW3(63)とWM検出手段(64)、MPEG符号化手段(65)を同一のLSI内に組み込むことにより、データを途中から取り出すことを困難にし、記録手段1(52)と切り替えSW4(53)、認証手段2d(55)、認証手段3d(56)は同一のLSI内に組み込むことにより、データを途中から取り出すことを困難にする。

【0035】図6は本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。本実施例は図1で示した実施例で、データバスと認証バスを独立に示したものを、兼用化した場合についての実施例である。図1と同じ番号のものは同じ物を示す。

【0036】図6において、70は1本化されたデータバス、71は1本化された認証バス、72は認証ブロック1の認証手段を切替えるSW、73は認証ブロック2の認証手段を切替えるSWである。このような構成とすることで、データバス、認証バスを兼用化し、デバイス間の接続線の数を削減することが出来る。

【0037】図7は本発明によるデータ再生装置をDVDドライブ装置に当てはめ、その出力信号を別のデバイス、例えばハードディスクのような記録可能なデバイスへ接続する場合を示したものである。本実施例は例えばハードディスクのような記録再生可能な記録媒体について示すが、勿論これはハードディスクのような記録再生可能な媒体全般に限定するものではなく、データバスを介してデータの受け渡しを行う装置全体にあてはまる。同図において、80はハードディスク装置、81はデータ記録装置1、82はシステム制御手段3、83はハードディスクである。

【0038】DVDディスク24からピックアップ26で読み出された信号はプリアンプ27を介してデータ再生装置1に入力される。データ再生装置1はシステム制御手段1により制御され、動作の状態を決定する。ここまでするDVDドライブ25の主な動作である。データ再生装置1で再生された信号は、データ記録装置1に伝送される。データ記録装置1はシステム制御手段3により制御され、記録動作の状態を決定する。データ記録装置1で再生されたデータは、ハードディスク83にデータが記録される。ここまでするハードディスク装置80の主な動作である。

【0039】ここで、データを記録することが出来る機器に関しては、コピー制御情報に従って記録制御を行う必要がある。そのため、正しく記録を制御する機能を備えた機器であるかどうかを確認するために、データ再生装置1からデータ記録装置1に対して認証を行う必要がある。データ再生装置1からデータ記録装置2へ受け渡すデータは、データを保護する場合にはスクランブルをかけて送るようにする。そのため、データ再生装置1及



びデータ記録装置 2 には、スクランブルをかける手段、スクランブルを解く手段、スクランブルのための鍵の受け渡しを行う手段を備えている。仮に、認証に失敗した場合には、データ再生装置 1 からデータ記録装置 2 へデータを出力しないようにし、もし、データを出力しても、スクランブルがかかっている、鍵の受け渡しができないため、データを正しく再生することが不可能となる。よって、スクランブルがかかったデータをそのまま記録装置で記録しても、正しく再生できなくなる。

【0040】また、ここでは、記録装置とのデータの受け渡しを行う場合についてのべたが、再生もしくは出力装置に場合にも同様に、正しくコピー制御を行う装置かどうかを認証して、データの保護を行うようにする。

【0041】このような手段を備えて、データの受け渡しを行うようにすることで、著作権などの権利のあるデータのコピー制御を正しく行い、不正なコピーや再生を防止することが可能となる。

【0042】図 8 は本発明によるデータ出力装置をモニタに当てはめた場合を示したものである。本実施例は例えばモニタのような出力について示すが、勿論これはモニタに限定するものではなく、データバスを介してデータの受け渡しを行う装置全体にあてはまる。同図において、90 はモニタ、91 はデータ処理装置 3、92 はコンバータ、93 は表示装置である。

【0043】MPEG ボード 29 からモニタ 90 に出力される。モニタ 90 で入力されたデータはコンバータ 31 で変換されて、モニタ 32 に出力し映像が映し出される。ここまではモニタの主な動作である。

【0044】ここで、データがデータバス 100 を介してモニタ 90 に入力される場合、不正に記録されないように保護するために、データにスクランブルがかかっている場合があり、その場合には、データ処理装置 3 でスクランブルを解いてコンバータ 92 へ出力するようにする。よって、この場合には、データ処理装置 3 の中に、MPEG ボード 29 に対応した認証処断を備えることが必要となる。また、MPEG ボード 29 からの出力がモニタ 90 のような表示装置のみに出力し、記録装置に出力しないことを確認するための認証を行うこともあり、記録装置の接続が無い場合には、データを不正にコピーされることがないため、モニタ 90 に出力する時に、データにスクランブルをかける必要はない。

【0045】このような手段を備えて、データの受け渡しを行うようにすることで、著作権などの権利のあるデータのコピー制御を正しく行い、不正なコピーや再生を防止することが可能となる。

【0046】図 9 は、上述した再生装置や記録装置等のデータ処理手段（以下「デバイス」という）を複数備えたシステムとしてのデータ処理装置、例えばパーソナルコンピュータの場合を示したものである。パーソナルコンピュータでは、各デバイスの組み込みを容易に変更で

きるので、本実施例に示した組み合わせに限定されるものではなく、データの受け渡しを行う全てのデバイスの組み合わせが含まれる。

【0047】同図の 101 は MPEG ボード、102 は MO ドライブ、103 はデジタルカメラである。

【0048】パーソナルコンピュータでは、データバス 100 を介して、各デバイスとの間でデータの受け渡しが行われる。その時に、データバス上で不正にコピーされることを防止するため、データバスに接続しているデバイスとの間で認証を行う。

【0049】ここで、認証が成立しなかった場合には、そのデバイスが正しくコピー制御を行う機能を備えていない機器であると判断して、データを出力することを止める。また、この時、再生だけが認められているデータである場合には、データバスに記録デバイスが接続されておらず、再生機能を持つ機器だけの場合には出力することも可能である。

【0050】また、認証が成立なかった場合には、受け渡すデータがコピー制限が無いものに限ってデータバス上を介してデータを受け渡すことができるようにしてもよい。

【0051】これらの認証は、各デバイスに備えられている回路により行うことも可能であるが、パーソナルコンピュータ等のような場合には、各デバイスを制御するためのソフトウェアにより、認証を行うことも可能である。また、各デバイスを統括的にコントロールする OS 上で認証を行い、その認証結果に応じて、各デバイスを制御するようにすることも可能である。

【0052】このようにデータバスに接続する各デバイス間で、データの種類に応じて認証を行い、その結果に従って、データの受け渡しを制御するようにすることで、正しくコピー制御を行うことを可能とした。

【0053】図 10 は本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。図 10 は、図 1 に示したものが、例えば、民生用 DVD プレーヤーのように、一つの機器の中で構成されているときの例を示したものである。このような機器の場合、DVD ドライブと MPEG ボードを組み替えることは困難なため、認証を行う必要はない。また、これら DVD 信号処理と MPEG デコードが同一の LSI 内部の処理として行われる場合にも、他に接続されたり、信号をデータバスの取り出したりされることはないため、認証は必要なくなる。これらの場合には、認証手段を複数持つことはなく、暗号の解読手段を複数切り替えて再生するようにする。

【0054】

【発明の効果】本発明によれば、記録媒体の種類とコピー制御の情報によって、異なるスクランブルがかけられたデータの再生を行なう場合に、それぞれに対応した認証手段を切り替えて用いることにより、スクランブルに

\* 【図 7】本発明によるデータ再生装置をDVDドライブ装置に当てはめ、その出力信号をハードディスクのような記録可能なデバイスへ接続する場合を示したものである。

【図 8】本発明によるデータ出力装置をモニタに当てはめた場合を示したものである。

【図9】本発明による各デバイスを備えたシステム、例えばパーソナルコンピュータの場合を示したものである

10 【図１０】本発明によるコピー制御情報を含むデータを再生する再生装置の別の実施例を示したものである。

【符号の説明】

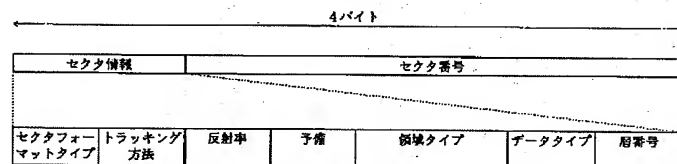
1…データ再生装置1、2…再生手段1、3…切り替えSW1、4…認証手段1a、5…認証手段2a、6…認証手段3a、7…データ再生装置2、8…認証手段1b、9…認証手段2b、10…認証手段3b、11…暗号解読手段1、12…暗号解読手段2、13…切り替えSW2、14…WM検出手段、15…MPEG再生手段、16…データ入力、17…データ出力、18…データバス1、19…認証バス1、20…データバス2、21…認証バス2、22…データバス3、23…認証バス3。

1、19…認証バス1、20…データバス2、21…認証バス2、22…データバス3、23…認証バス3。

1、19…認証バス1、20…データバス2、21…認証バス2、22…データバス3、23…認証バス3。

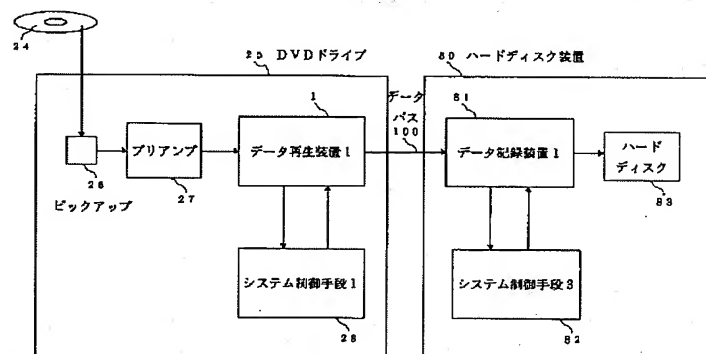
1、19…認証バス1、20…データバス2、21…認証バス2、22…データバス3、23…認証バス3。

【图 4】



【图7】

图 7



【図1】

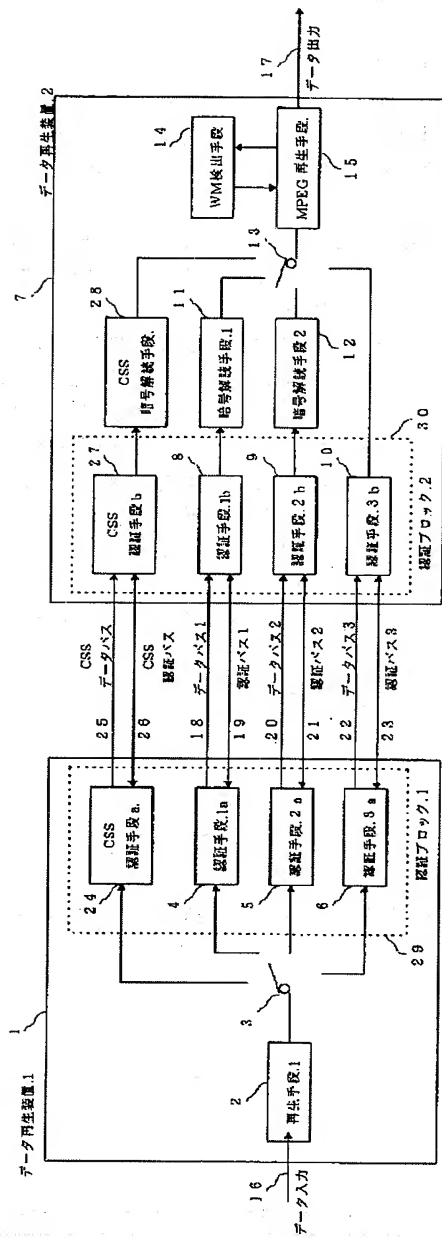


図1

【図6】

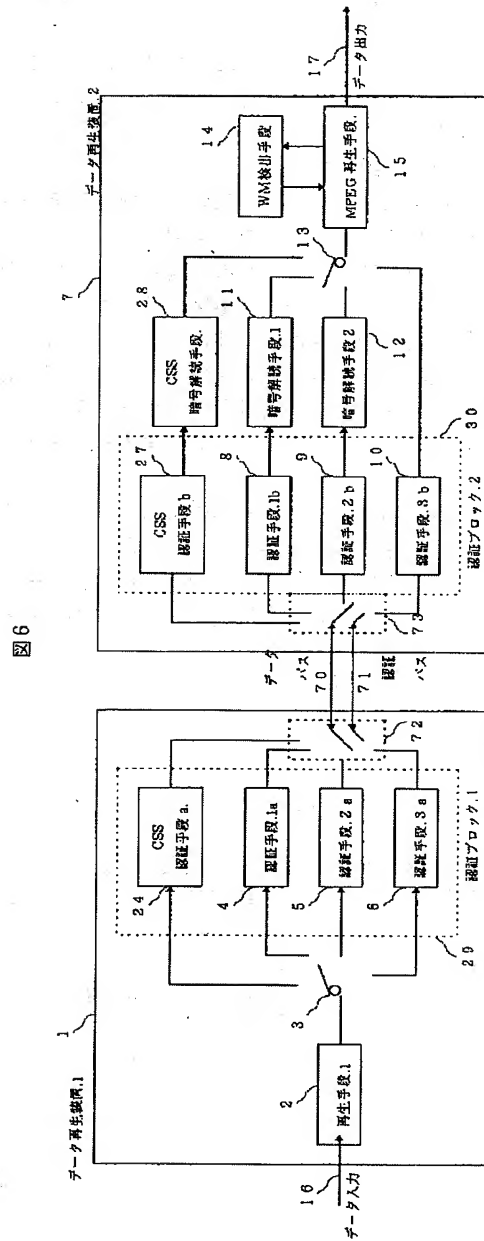
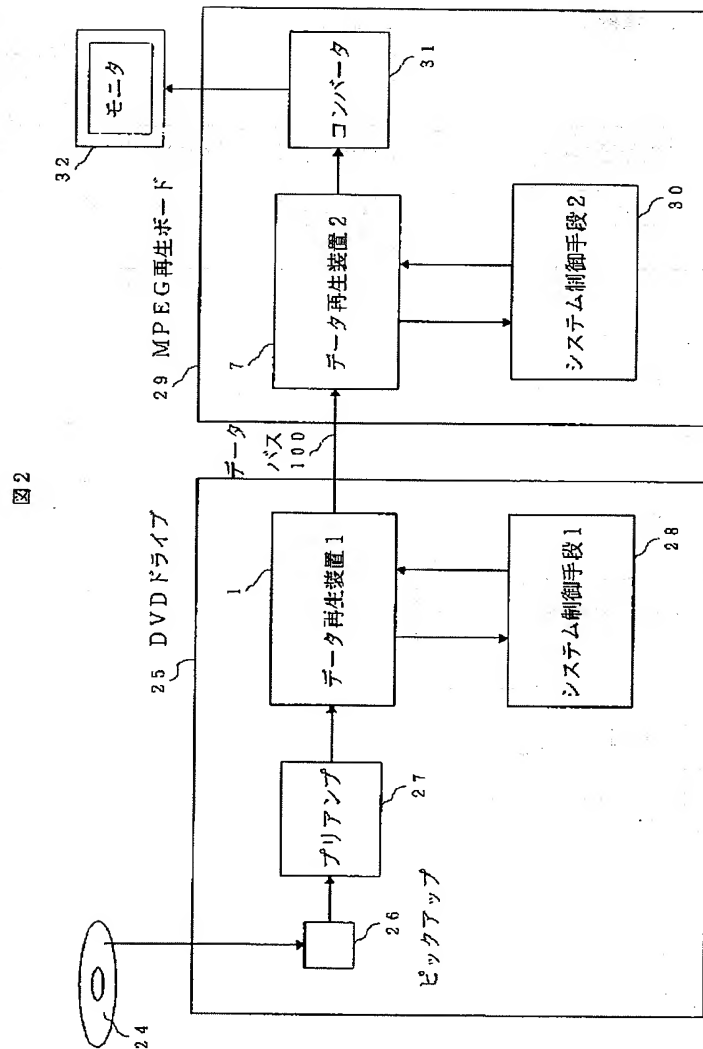


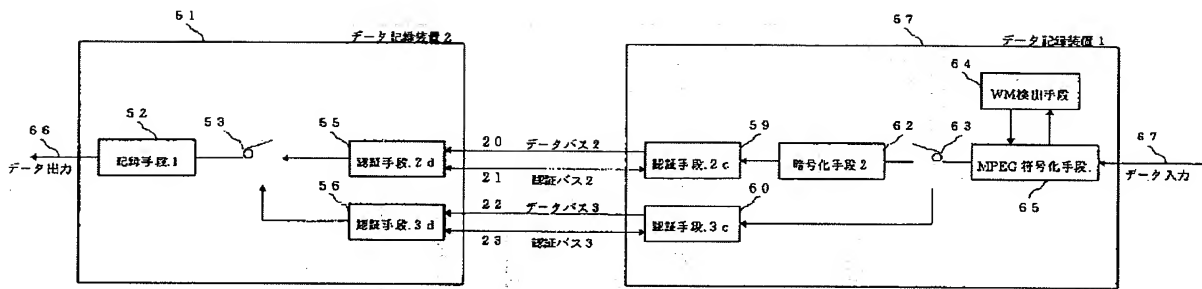
図6

【図2】



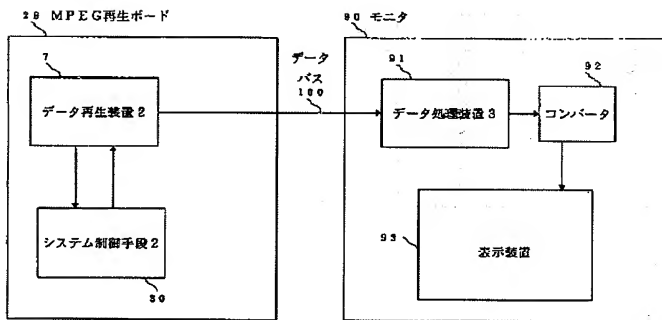
【図5】

図5



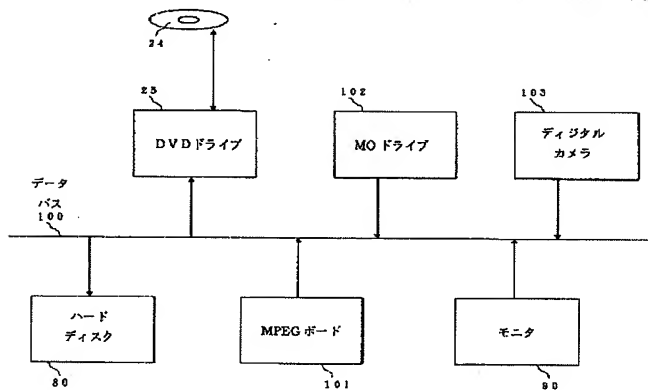
【図8】

図8



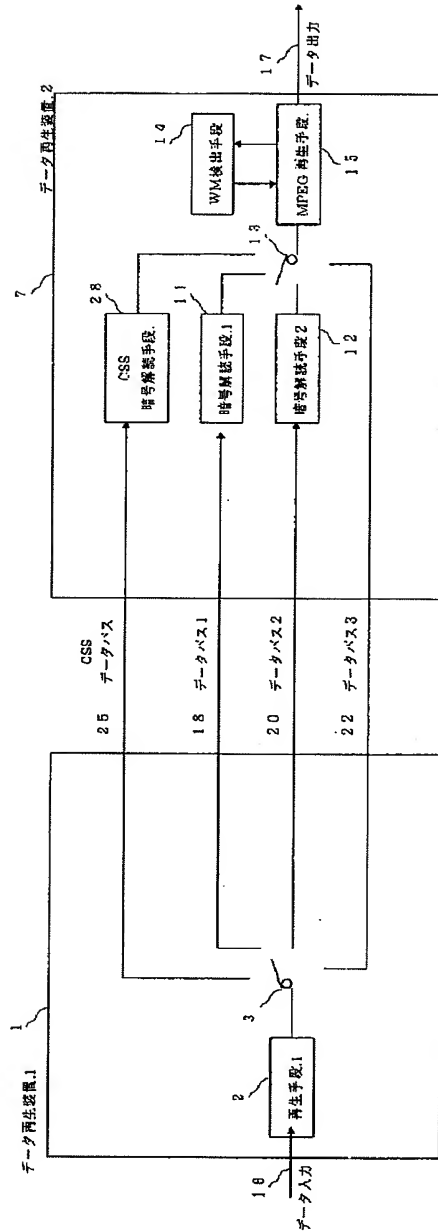
【図9】

図9



【図10】

図10



フロントページの続き

(51)Int. Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

(72)発明者 荒井 孝雄  
 神奈川県横浜市戸塚区吉田町292番地株式  
 会社日立製作所情報メディア事業本部内

(72)発明者 木村 寛之  
 神奈川県横浜市戸塚区吉田町292番地株式  
 会社日立製作所情報メディア事業本部内

(72)発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地株式  
会社日立製作所システム開発研究所内



【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第4区分

【発行日】平成17年6月9日(2005.6.9)

【公開番号】特開2001-236729(P2001-236729A)

【公開日】平成13年8月31日(2001.8.31)

【出願番号】特願2001-8431(P2001-8431)

【国際特許分類第7版】

G 1 1 B 20/10

H 0 4 N 5/91

H 0 4 N 5/92

H 0 4 N 7/167

【F I】

G 1 1 B 20/10 H

H 0 4 N 5/91 P

H 0 4 N 5/92 H

H 0 4 N 7/167 Z

【手続補正書】

【提出日】平成16年9月3日(2004.9.3)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】再生装置、データ記録装置、記録再生装置、表示装置、記録再生方法、および暗号解読装置

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

記録媒体から再生したデータを出力して外部装置に記録する再生装置において、前記外部装置は複数の暗号化手段と認証手段を備え、複数の暗号化手段の中から前記記録媒体から再生したデータの種類に対応した暗号化手段を選択して暗号化し、前記暗号化されたデータに対応した認証手段を選択して前記外部装置との認証を行い、認証が確認された後に、前記外部装置に記録するデータを出力することを特徴とする再生装置。

【請求項2】

記録媒体から再生装置によって再生され出力されたデータを、入力して記録するデータ記録装置において、前記データ記録装置は、複数の暗号化手段と認証手段を備え、前記記録媒体から再生されたデータの種類に対応した暗号化手段を選択して暗号化し、前記暗号化されたデータに対応した認証手段を選択して前記再生装置との認証を行い、認証が確認された後に、前記再生装置から出力されるデータを入力し、当該入力されたデータを記録することを特徴とするデータ記録装置。

【請求項3】

互いに認証し合うことによりデータの授受を行ってデータを記録または再生する複数のデータ記録再生装置またはデータ再生装置を有する記録再生装置であって、前記複数のデータ記録再生装置またはデータ再生装置は、それぞれ複数の暗号化手段と認証手段を有し

、前記記録再生装置は、前記データの種類に対応した暗号化手段を選択して暗号化し、前記複数のデータ記録再生装置またはデータ再生装置が有する認証手段の中から前記暗号化されたデータに対応した認証手段を選択して、認証することを特徴とする記録再生装置。

【請求項 4】

請求項 3 に記載の記録再生装置において、  
前記認証はソフトウェアにより行うことを特徴とする記録再生装置。

【請求項 5】

請求項 4 に記載の記録再生装置において、  
前記認証は、複数のデータ記録再生装置またはデータ再生装置を統括的に制御するプログラムにより行うことを特徴とする記録再生装置。

【請求項 6】

請求項 3 に記載の記録再生装置において、  
前記複数の暗号化手段は前記データが映像信号か音声信号か静止画画像信号かプログラムのコードかまたはそのいずれでもないかの種類を示す情報によって選択されることを特徴とする記録再生装置。

【請求項 7】

請求項 3 に記載の記録再生装置において、  
前記複数の暗号化手段は前記データに含まれたコピーを制御するための情報によって選択されることを特徴とする記録再生装置。

【請求項 8】

請求項 3 に記載の記録再生装置において、  
前記複数のデータ記録再生装置またはデータ再生装置のうち、少なくとも一つは可換な記録媒体を扱う装置であることを特徴とする記録再生装置。

【請求項 9】

請求項 3 に記載の記録再生装置において、  
前記複数のデータ記録再生装置またはデータ再生装置のうち、少なくとも一つは可換でない記録媒体を扱う装置であることを特徴とする記録再生装置。

【請求項 10】

請求項 8 に記載の記録再生装置において、  
前記複数の暗号化手段は前記記録媒体の種類を示す情報によって選択されることを特徴とする記録再生装置。

【請求項 11】

請求項 9 に記載の記録再生装置において、  
前記複数の暗号化手段は前記記録媒体の種類を示す情報によって選択されることを特徴とする記録再生装置。

【請求項 12】

請求項 3 に記載の記録再生装置において、  
前記複数のデータ記録再生装置またはデータ再生装置の組み合わせが可換でない場合には、  
前記データに対応した暗号を解く鍵の受け渡しを行うことを特徴とする記録再生装置。

【請求項 13】

データを入力して表示する表示装置において、前記表示装置は複数の暗号解読手段と認証手段を備え、複数の暗号解読手段の中から入力されたデータの種類に対応した暗号解読手段を選択し、入力したデータに対応した認証手段により、入力されたデータを出力した出力装置との認証を行い、認証が確認された後に、前記出力装置から出力されるデータを入力し、当該入力されたデータを表示することを特徴とする表示装置。

【請求項 14】

記録媒体から再生され、出力されたデータを入力して表示する表示装置において、前記表示装置は複数の暗号解読手段と認証手段を備え、複数の暗号解読手段の中から、前記記録媒体から再生されたデータの種類に対応した暗号解読手段を選択し、入力したデータに

対応した認証手段により前記データ再生装置との認証を行い、認証が確認された後に、前記データ再生装置から出力されるデータを入力し、当該入力されたデータを表示することを特徴とする表示装置。

【請求項 15】

請求項 13 に記載の表示装置において、前記表示装置と前記データを出力した再生装置は、それぞれ複数の暗号解読手段を有し、前記複数の暗号解読手段は前記データが映像信号か音声信号か静止画画像信号かプログラムのコードかまたはそのいずれでもないかの種類を示す情報によって選択されることを特徴とする表示装置。

【請求項 16】

請求項 13 に記載の表示装置において、前記表示装置と前記データを出力した再生装置は、それぞれ複数の暗号解読手段を有し、

前記複数の暗号解読手段は前記データに含まれたコピーを制御するための情報によって選択されることを特徴とする表示装置。

【請求項 17】

請求項 14 に記載の表示装置において、前記表示装置とデータを出力したデータ再生装置は、それぞれ複数の暗号解読手段を有し、

前記複数の暗号解読手段は前記データに含まれた記録媒体の種類を示す情報によって選択されることを特徴とする表示装置。

【請求項 18】

請求項 14 に記載の表示装置において、前記表示装置とデータを出力したデータ再生装置は、それぞれ複数の暗号解読手段を有し、

前記複数の暗号解読手段は前記データに含まれた記録媒体の種類を示す情報とコピーを制御するための情報との組み合わせによって選択されることを特徴とする表示装置。

【請求項 19】

請求項 18 に記載の表示装置において、前記記録媒体の種類を示す情報は、再生専用の媒体か記録可能な媒体かを示す情報を備え、前記コピーを制御するための情報は、コピー制限がないか、コピー禁止か、一世代だけコピー可能かを示す情報を備えていることを特徴とする表示装置。

【請求項 20】

請求項 18 に記載の表示装置において、

前記組み合わせは少なくとも、再生専用の媒体であるとの情報と、記録可能な媒体であってかつコピー禁止か一世代だけコピー可能かを示す情報と、記録可能な媒体であってコピー制限がないとの情報という 3 種類の組み合わせを有することを特徴とする表示装置。

【請求項 21】

それぞれ複数の暗号化手段を有し互いに認証し合うことによりデータの授受を行ってデータを記録再生する複数のデータ記録再生装置またはデータ再生装置を有する記録再生装置における記録再生方法であって、

前記複数のデータ記録再生装置またはデータ再生装置は、前記データの種類に対応した暗号化手段をそれぞれ選択し、かつ、相互に認証し合うことを特徴とする記録再生方法。

【請求項 22】

暗号化されたデータを入力して再生する暗号解読装置であって、前記暗号化されたデータの暗号を解除する複数の暗号解読手段と、前記暗号解読手段により解読されたデータを再生する再生手段とを有し、

前記複数の暗号解読手段のうち、前記暗号化されたデータの種類に対応した暗号化手段を、入力されたデータから選択して、前記暗号化されたデータの暗号を解除することを特徴とする暗号解読装置。

【請求項 23】

請求項 22 に記載の暗号解読装置において、

前記複数の暗号解読手段は前記データが映像信号か音声信号か静止画画像信号かプログラムのコードかまたはそのいずれでもないかの種類を示す情報によって選択されることを特徴とする暗号解読装置。

【請求項 24】

請求項 22 に記載の暗号解読装置において、  
前記複数の暗号解読手段は前記データに含まれたコピーを制御するための情報によって選択されることを特徴とする暗号解読装置。

【請求項 25】

請求項 22 に記載の暗号解読装置において、  
前記複数の暗号解読手段は前記データに含まれた記録媒体の種類を示す情報によって選択されることを特徴とする暗号解読装置。

【請求項 26】

請求項 22 に記載の暗号解読装置において、  
前記複数の暗号解読手段は前記データに含まれた記録媒体の種類を示す情報とコピーを制御するための情報との組み合わせによって選択されることを特徴とする暗号解読装置。

【請求項 27】

請求項 22 に記載の暗号解読装置において、  
前記記録媒体の種類を示す情報は、再生専用の媒体か記録可能な媒体かを示す情報を備え、  
前記コピーを制御するための情報は、コピー制限がないか、コピー禁止か、一世代だけコピー可能かを示す情報を備えていることを特徴とする暗号解読装置。